87107650

for 351799

Taiwan Patent Publication No. 351799

TRANSACTION METHOD WITH A MOBILE APPARATUS

The present invention relates to a method and a system for transmitting orders in a telecommunication network. The invention relates particularly, but not solely, to the transmission of orders in a mobile radio network.

According to the prior art, transactions between a client (C) and a terminal, here called point-of-transaction (POT), are often carried out by means of an electronic payment card. Debit and credit cards are used, for example, at cash desks in shops, service stations, etc. The card usually comprises storage means, e.g., a magnetic strip and/or a chip in which the identification of the client is stored, among others things. In order to carry out a transaction with the owner or operator of a POT, e.g., in order to pay for an article in a shop, the client must insert his card in a suitable card reader in the POT apparatus. The POT then reads the client's identification in the card, ascertains and displays the amount to be paid, checks the client's solvency, if need be, and prompts the client to confirm the transaction by means of a confirmation key on the POT apparatus. If the client is solvent and has entered his confirmation, the client identification, the amount to be paid, and possibly also a POT identification are transmitted over a telecommunication network to a financial server connected to the POT and administered by a financial institution. The client's account at this financial institution is debited accordingly either immediately or subsequently.

A drawback of this method is the necessity of having to insert the client's card in an outside apparatus. Clients do not normally have their cards handy but rather in their wallets, for instance; a very quick transaction is therefore not possible. Sometimes, too, the aperture for insertion of the card in the POT reading apparatus is not easily accessible; this is especially true when the POT is an automatic ticket dispenser for a parking garage or an automated payment machine which a motorist is supposed to be able to operate without getting out of his car. Moreover, fraudulent acts or the non-authorised reading of storage areas of the card may be carried out in the POT.

Even though certain chip cards contain a microprocessor nowadays, such debit and credit cards are substantially passive elements which store data memorised and used essentially by the electronics of the POT. The client, on the other hand, normally has no possibility of accessing the data directly without going to a teller's window or an automated teller machine of the respective financial institution which issued the card. Hence it is difficult for the client to check the transactions carried out by means of the card or to keep account of them.

Such cards contain a client identification, but one which permits the clients to be identified only to the issuing financial institution. Normally, therefore, a card can be used for a financial transaction only if the client and the POT operator are associated with the same financial institution. On the other hand, the card is not intended to be used for other types of transaction, e.g., for non-financial transactions where, however, reliable identification of the client or card-holder is needed. For the client, therefore, it is indispensable to have a large number of cards for all kinds of financial or non-financial transactions, e.g., several debit or credit cards administered by different financial institutions or chain stores, or subscriber cards or admission cards for protected zones. Such cards are usually protected by different PIN codes which the client must laboriously memorise.

In the event of theft or a fraudulent act involving the card, it must be blocked. However, blocking cannot take place until the card is inserted in a respective apparatus. Ordinary credit cards, though, can continue to be used in manually operated apparatus; hence secure blocking of the card is not possible.

Besides debit and credit cards, there are so-called e-cash cards which make it possible to store sums of money electronically and which are then accepted as payment means at various POT locations. In order to provide these cards with further sums, clients must present them at teller's windows or automated teller machines of a financial institution, and this is not always possible either.

An object of the present invention is to propose a method or system which allows these problems to be avoided.

A further object of the present invention is to propose a transaction method which is suitable for both financial and non-financial transactions and which is simpler and more reliable than the usual transaction methods.

According to the present invention, these objects are achieved particularly by means of a transaction method between a client and a fixed point-of-transaction apparatus (POT apparatus), the method comprising the transmission of at least one client identification, a POT apparatus identification (POSID), and transaction-specific data (A) to a server connected to said POT apparatus by means of a telecommunication network, characterised in that the POT apparatus identification (POSID) is read or entered in the POT apparatus and is transmitted to the server over said telecommunication network,

that the client is equipped with a portable identification element containing at least one processor and being capable of co-operating with a mobile apparatus for sending and/or receiving short messages by means of a mobile radio network,

and that the client identification (IDUI) is stored in the memory of the identification element and is transmitted to the server via at least one contact-free interface.

In addition, these objects are particularly achieved by means of a mobile system containing:

- at least one processor having a memory area in which a client identification (IDUI) is stored,

- electronic receiving means for receiving special short messages transmitted over a mobile radio network,

- electronic signing means for providing transaction vouchers containing at least one client identification (IDUI) with an electronic signature,

- a contact-free interface for forwarding the signed transaction vouchers to a POT apparatus.

The client identification is preferably linked to the POT apparatus identification entered or read in the POT apparatus and to data specific to the transaction in an electronic transaction voucher which is transmitted to the server by said telecommunication network and via a clearing unit.

The server may preferably communicate with the mobile system (e.g., a mobile apparatus having an identification card) via an air interface, e.g., a mobile radio network. When the transaction is a financial one, a further sum of money to be stored in the mobile apparatus can thereby be charged from the server by means of electronic messages transmitted via the air interface. The sum of money is preferably defined in a standard currency.

The contact-free transmission between the mobile system and the POT apparatus may, for example, take place through an electromagnetic interface integrated in the identification card or in the mobile apparatus, e.g., in the form of an inductive coil, or through an infrared transceiver system.

The transaction vouchers are preferably encoded by means of a symmetrical algorithm before they are forwarded to the server, the symmetrical algorithm using a session key encoded by means of an asymmetrical algorithm. Moreover, the transaction vouchers are preferably additionally certified before they are forwarded to the financial server. Preferably, a transmission link secured end-to-end between the mobile system and the financial server is ensured.

The present invention will be better understood with the aid of the following description and the accompanying drawings, in which:

Fig. 1 is a block diagram showing the information flow in a first embodiment of the inventive system, the client being equipped with a mobile radio telephone, preferably a GSM mobile apparatus which can receive and send special short messages;

Fig. 2 is a block diagram showing the information flow in a second embodiment of the inventive system, the client being equipped with a mobile radio telephone, preferably a GSM mobile apparatus which can receive and send special short messages, and the POT apparatus having Internet or Intranet capability;

Fig. 3 is a block diagram showing the information flow in a third embodiment of the inventive system, the client being equipped with a transponder capable of processing at least special short messages, and the POT apparatus being capable of receiving and/or sending special short messages, e.g., SMS or USSD short messages;

Fig. 4 is a block diagram showing the information flow in a fourth embodiment of the inventive system, the client being equipped with a transponder capable of carrying out at least some SICAP procedures, and the POT apparatus having Internet or Intranet capability and being capable of receiving and/or sending special short messages, e.g., SMS or USSD short messages;

Fig. 5 is a flow chart of an inventive payment transaction method;

Fig. 6 is a flow chart of an inventive transaction method for recharging a SIM card;

Fig. 7 is a block diagram showing the information flow in a fifth embodiment of the inventive system;

Fig. 8 is a block diagram showing the information flow in a sixth embodiment of the inventive system;

Fig. 9 is a block diagram showing the information flow in a seventh embodiment of the inventive system;

Fig. 10 is a block diagram explaining the signing of messages;

Fig. 11 is a block diagram explaining the verification of the signature;

Fig. 12 is a block diagram explaining the signing and verification of the signature;

Fig. 13 is a block diagram explaining the encoding of the messages.

The method illustrated in Figs. 5 and 6 can be carried out with any desired system shown in Figs. 1 to 4. The first and second modifications both require a mobile apparatus or a SIM card having an additional infrared or inductive interface, to be described in detail below.

Fig. 1 shows the information flow in a first embodiment of the invention. The client is equipped with a mobile system, in this case a GSM mobile apparatus 1. The mobile apparatus 1 contains an identification card 10, e.g., a SIM card, by means of which the client is identified in a network 6, preferably a GSM network. The SIM card comprises a conventional microcontroller 100 embedded in the plastic support body of the card and responsible for the GSM functionalities of the card--as they are described, for example, in the article "SIM CARDS," by T. Grigorova and I. Leung which appeared in the Telecommunication Journal of Australia, Vol. 43, No. 2, 1993, on pp. 33-38--and for new functionalities loaded on the SIM cards at a later date. The SIM card further comprises contact means (not shown) for communicating with the mobile apparatus 1 in which it is inserted.

The SIM card further comprises a second processor 101 (contact-free chip-card interface CCI) responsible for the contact-free connection to a POT apparatus 2. The second process carries out, among other things, the TTP (trusted third-party) functions to be described below in order to receive

and send coded and signed messages. A logic interface 102 connects the two processors 100 and 101.

The contact-free interface with the POT apparatus 2 may, for example, comprise at least one coil (not shown), integrated in the SIM card and connected to the second processor 101, by means of which data are inductively transmitted in both directions over a radio communication route. As a modification, an inductive coil may also be integrated in the housing of the mobile apparatus. As a third modification, the contact-free interface comprises an infrared transceiver on the housing of the mobile apparatus. The contact-free communication between the two apparatus is preferably encoded, e.g., by means of a DEA, DES, TDES, RSA, or ECC security algorithm.

For inductive signal transmission from the POT to the chip card, a phase-modulation process is preferably utilised, whereas in the opposite direction it is preferably the amplitude of the signals which is modulated.

The SIM card preferably contains a special field IDUI (international debit user identification) by means of which the client is identified by the POT operator and/or by a financial institution. The IDUI identification is preferably stored in a protected memory area of one of the two processors 100, 101.

The IDUI contains at least an identification of the network operator, a user number which identifies him from other clients with the same network operator, a user class indication which defines which services he may use, and optionally also a country identification. Moreover, the IDUI contains security data, including a transaction counter Tc, a charging token CTc1 , and a time-out field TO indicating the validation time. The function of these various data will be explained below.

The symbolically depicted POT apparatus 2 is likewise provided with a contact-free transceiver 20, e.g., an inductive coil or an infrared transceiver. Owing to this interface, the mobile system 1, 10 can communicate contact-free with the apparatus 2 in both directions.

The terminal or POT apparatus 2 may, for example, be a point-of-sale (POS) in a shop, specially equipped with a radio communication interface 20. However, the POT apparatus 2 may also be intended for non-financial applications, e.g., as a code for an admission-checking device ("electronic gatekeeper") which permits coming and going in a protected locality, e.g., a hotel room, business, theatre, cinema, or within an amusement park. The POT apparatus is identified by means of a special field POSID (point-of-sale identification). The POSID depends upon the application; in the case of a cash desk, it contains an identification of the network operator, an area identification (sub-district in a country), a POS number identifying it from other POS with the same network operator, a POS class indication defining what services it may use or offer, the date, time, currency used (SDR, euros, or dollars), and optionally a country identification as well.

The POT apparatus 2 is preferably provided with data-entry means (not shown), e.g., a keypad, and with display means (not shown), e.g., a screen.

The IDUI identification is transmitted to the POT via the contact-free interface 10/101 and linked in the POT apparatus to the POSID and to additional data specific to the transaction, e.g., the debit amount A entered, so that an electronic transaction voucher is created which is encoded by means of a TTP (trusted third-party) or PTP (point-to-point) process and signed. Additional explanations concerning the TTP process are given below in an appendix.

The transaction voucher is then transmitted via a modem (not shown) and a communication network 5, e.g., a public fixed network 5 or a mobile radio network, to a clearing unit 3 likewise connected to the network. The unit 3 receives the electronic vouchers from various POT apparatus 2, independently of the country or traffic area, and independently of the country or financial institution of the client. In the clearing unit 3, these transaction vouchers are arranged according to financial institution, possibly also according to operator, and sent to the respective financial institutions. Clearing units are already known per se in GSM technology and are used, for instance,

for collection and further distribution of connection charges. The clearing unit may, for example, contain a data base indicating the financial institution with which the client previously identified by means of his IDUI is associated.

The electronic transaction vouchers handled by the clearing unit 3 are forwarded to a financial server 4, 4', or 4" of the respective financial institution. In the financial server, the transaction vouchers submitted are first decoded and stored in an intermediate memory 43. A squaring management module 42 then credits the amount signed by the client to the respective bank accounts 420, 420', and/or 420" of the POT operator. These accounts may be administered by the same or a different financial institution. Moreover, the squaring management module carries out checking entries in the client's account. The client's account 41 with the financial institution is debited accordingly, or the transaction data are stored for later checking. The financial server further contains a TTP server 40 for encoding and signing vouchers and messages by means of the TTP (trusted third-party) algorithm. Additionally, each financial server 4 is connected to a SIM server 70, e.g., to a SICAP server. The SICAP process has been described in European Patent No. 689,368, for example, and enables the exchange of files, programs, and also sums of money between the SICAP server 70 and the SIM card 10 in the mobile apparatus 1 over the public GSM network 6 (arrow 60). Other transmission protocols may also be used for data transmission between the SIM server and the SIM cards. For instance, the SIM card 10 can be recharged thereby, as described in detail below. The SIM server 70 further makes possible controlled communication between the client and the TTP server 40 at the financial institution.

Fig. 2 shows the information flow in a second embodiment of the invention. In this modification, too, the client is equipped with a mobile system, e.g., a GSM mobile radio telephone 1 having a SIM card, preferably a SIM card having SICAP capability. The mobile system 1 likewise contains an inductive or infrared interface by means of which a contact-free connection to the POT apparatus 2 can be carried out. In this way, data and/or programs can be exchanged in both directions between the POT apparatus 2 and the SIM card 10 in the mobile system.

In this case, however, the POT apparatus 2' is a computer, preferably connected to a network, e.g., on the Internet or in an Intranet. Various types of information or offers, e.g., offers of products, may be displayed on the monitor of the computer 2 by means of a suitable menu. The client can control this computer with his mobile apparatus. For example, he can control the position of a cursor in a menu of products or information offered for sale by operating the cursor-shifting keys on the keypad 11 of his mobile telephone. The cursor-shifting instructions are transmitted to the computer 2' via the contact-free interface 101, 20. The user presses a confirmation key, e.g., the #-key on his keypad, in order to confirm the selected menu option, e.g., to order a product.

The client identification stored in the mobile system 1, 10 is linked in an electronic transaction voucher to the POT apparatus identification and to the transaction-specific data corresponding to the selected menu option, TTP or PTP encoded, and signed. The transaction voucher preferably contains a client identification IDUI extracted from the SIM card 10, a supplier identification corresponding to the selected menu option, and a product identification corresponding to the selected menu option, preferably in the Flexmart format as proposed in International Patent Application PCT/CH96/00464. This voucher is established by a Flexmart module 21. The Flexmart module is preferably a software application run by the computer 2'.

Analogously as in the first embodiment, the electronic transaction voucher is then transmitted by the clearing unit 3 to the respective financial server 4, 4', or 4" and processed there.

Fig. 3 shows the information flow in a third embodiment of the invention. In this modification, the client is not equipped with a complete mobile apparatus but only with a transponder 10' which may be integrated in a chip card, for instance, or in any object, such as a watch, a ring, or a keyring. The transponder might also be integrated in a remote control, e.g., an infrared remote control, and communicate with the POT apparatus 2 via this remote control. The transponder 10' contains a first processor 100' by means of which special short messages, e.g., SMS or USSD short messages, can be sent

received, and encoded. In a preferred modification, the first processor 100' contains SICAP and/or TTP modules by means of which files and programs can be exchanged with a server 7 by SMS or USSD short messages. However, the first processor 100' does not contain any mobile radio functions, hence the transponder cannot be used as a SIM card in a mobile radio apparatus.

A second chip 101 (contact-free chip-card interface, CCI) is connected to the chip 100' through an interface 102 and is responsible for the contact-free connection to the apparatus 2. It is naturally also possible to use a single chip performing both functions. In this case, the contact-free connection preferably takes place by means of at least one inductive coil in the transponder 10'.

The POT apparatus 2" comprises in this case a transceiver 20 for contact-free communication with the transponder 10', data-processing means 23 having a keypad 11, and a mobile radio apparatus 24, preferably a reduced GSM apparatus which can receive and send only special short messages, such as SMS or USSD short messages. The keypad is used by the client as an input means.

The GSM apparatus 24 integrated in the POT apparatus and reduced to the transmission of short messages makes possible the transmission of messages through the mobile radio network 6 between the transponder 10' and a first application in the SIM server 7, and thereby the encoded recharging and/or check-up process (arrow 60) and the voucher transfer (arrow 61) from the client to a SIM server application 71 in the SIM server 7, e.g., in a SICAP server. As a modification, the encoded recharging and/or check-up process and the voucher transfer may also take place via a modem or an ISDN connection 22 and a fixed network 5.

The messages and vouchers are then transmitted by the mobile radio network 6 via the contact-free interface 101/20 and over the mobile radio route 60, 61.

Fig. 4 shows the information flow in a fourth embodiment of the invention. As in the third modification, the client is not equipped with a complete mobile apparatus but only with a transponder 10'. As in the second embodiment, the POT apparatus 2''' is connected to data-processing means 2' having a Flexmart module 21. The client communicates with the SIM server 7 by means of a restricted mobile radio apparatus 24, e.g., a GSM apparatus 24 in the apparatus 2''', reduced to the transmission of special SMS or USSD short messages. The other functions are analogous to those of the third embodiment.

By means of the Flexmart module 21, order messages may be prepared in a standardised format for a product or information supplier, as described in International Patent Application PCT/CH96/00464.

A payment transaction method will now be described in detail with the aid of Fig. 5. This method may be applied to any of the embodiments of the invention illustrated in Figs. 1 to 4. However, this sequence of operations is generally applicable and not limited to GSM processes.

The first column in Fig. 5 shows the process steps involving chiefly the client's mobile system 1; the second column describes the process steps carried out by the POT apparatus 2; the third column relates to the operations of the financial server 4, and the fourth to the effects upon the various accounts at the financial institution. It must be noted, however, that many process steps may be carried out either with the mobile system 1, e.g., as a process within the SIM card 10, or in the POT apparatus 2. For example, the data input may take place by means of either the POT or the mobile system 1 if the latter has a keypad, such as a GSM mobile apparatus.

This method presupposes in step 200 that the client's identification card 10, here a value card, is credited with a sum of money (e-cash). Value cards are already known per se; how they may be recharged will be explained in detail below with reference to Fig. 6. Moreover, PCT Application WO 98/09255 describes a method of recharging a SIM card.

The mobile system 1 or 10 is switched into operational state, e.g., by switching on the mobile apparatus, in step 201. The POT apparatus 2 is likewise activated in step 202. The POT apparatus 2 then calls up in step 201 in a broadcast process the next, indeterminate client (card paging).

When the connection has been established between the POT apparatus and the mobile system 1, 10, the mobile system furnishes to the POT apparatus in step 204 the client's IDUI (international debit user identification) and the confirmation that he is solvent. Whether the solvency is adequate cannot yet be determined at this time.

The POT apparatus 2 contains a blacklist, preferably updated periodically by the financial server 4, of clients to be barred. The IDUI transmitted by the client is compared with the blacklist (step 205). If the IDUI furnished by the client is found in the blacklist (step 206), a blocking flag is set in step 207. If no entry is found, the data specific to the transaction, e.g., a debit amount A to be paid, may be entered on the keypad 11 of the POT apparatus 2. As a modification, the amount A may also be entered on the keypad of the mobile apparatus 1. The POT apparatus 2, or in a modification the SIM card 10, then links these transaction-specific data with the identification of the POT apparatus 2 and the IDUI and sends this debit order to the client. In addition, a reference currency, such as SDR, euros, or dollars, is preferably included as well.

Since the communication is signed, it can be checked in step 210 whether the debit order correlates with the IDUI. If not, the reason for rejection is displayed on the POT apparatus 2 (step 223). Otherwise, a blocking flag is checked in step 211. If one is set, a check-up with the financial server 4 takes place (step 248). If none is set, an area check-up takes place (step 213). SIM cards may thereby be blocked according to area of use. If the area check-up is negative, a check-up with the financial server 4 takes place (step 248); otherwise, a time-out check-up is made (step 215). It is checked whether the validation time during which transactions may be carried out without check-up has already expired. If the validation time has expired (216), a check-up with the financial server takes place (step 248); otherwise, the client is prompted

step 217 to enter his user password manually on the mobile apparatus 1. If the password entered is correct (step 248), the amount A is converted (219), if need be, into the uniform currency (say, SDR). This makes possible international utilisation of the concept. Otherwise, in step 223, the rejection is displayed on the POT apparatus 2 with indication of the reason.

The mobile system 1/10 then checks in step 220 whether the amount A to be debited is covered by the sum of money credited on the card (solvency check). If not, this reason for rejection is displayed on the screen of the POT apparatus (step 223).

When all these checks have taken place, the transaction is counted in step 222 by means of a transaction counter Tc which is incremented. This count corresponds to the number of transactions executed with the card 10. In step 224, the debit amount A, the POT apparatus identification POSID, and the user identification IDUI are then linked in a transaction voucher which is additionally certified, optionally encoded, and possibly also compressed. The ECC method (elliptic curve crypto system), for example, may be used for the certification. A suitable certification and encoding method will be described in detail below.

The debited amount A is deducted from the card account in step 225, and the transaction voucher is filed in step 226 in a stack on the identification element 10. This card stack of the client's can be retrieved by the financial server, if necessary, for the purpose of a detailed check. Preferably, the client himself can display the transaction vouchers stored in the stack on his mobile apparatus.

After step 224, the transaction voucher is supplied to the POT apparatus 2 for settlement, and the signature is verified by the POT apparatus (step 227). Optionally, in step 228, a voucher is printed out on paper for the client.

In step 229, the debit voucher is then linked in the POT apparatus 2 with any additional POS data, and the transaction voucher is electronically

signed by the POT apparatus, and optionally compressed and encoded. The electronic transaction voucher prepared in this way is then optionally filed in step 230 in a stack in the POT apparatus 2. The stack contains transaction vouchers of various clients. The transaction vouchers are then transmitted individually or in groups to the clearing unit 3 during step 231. Transmission may take place either immediately after the transaction, or a number of transaction vouchers may be transmitted from the stack at periodic intervals (e.g., every hour or every day). A batch process for transmitting all transaction vouchers during the night, for instance, may also be used.

The clearing unit 3 receives individual or grouped transaction vouchers from a plurality of POT apparatus 2 in the same geographical zone (step 234). A plurality of geographically distributed clearing units may be provided. In step 235, the clearing unit 3 assigns the transaction vouchers received from various POT apparatus to the respective financial institutions or service providers and forwards these transaction vouchers accordingly.

If the transaction vouchers are encrypted, they must first be decoded by the clearing unit in order to be assigned to a financial server 4, 4', 4", then re-encrypted by the clearing unit in order to be forwarded. In a preferred modification, however, the data elements in the fields IDUI and possibly POSID of the transaction voucher, needed for clearing, are not encrypted by the POT apparatus 2. Secure, end-to-end encoded transmission of the transaction vouchers between the POT apparatus and the financial servers 4, 4', 4" can thereby be achieved.

The responsible financial server receives the transaction vouchers in step 236, and the TTP server 40 decompresses and decodes them (if necessary) and verifies the authenticity of the signatures of the POT apparatus and of the client. In step 237 it is checked whether the POSID and/or the IDUI are to be found on a revocation list. If the test is negative (238) because neither the POT apparatus identification nor the client identification IDUI is on a revocation list, a test of the charging token CT takes place in step 239. The charging token CT gives the number of times the card 10 has been recharged. This charging token is updated in the financial server (CTs) and in the card

(CTc) after each recharging process, as described below. A copy of the charging token CTc is transmitted in the field IDUI in the transaction voucher. The charging token CTc communicated by the mobile system 1, 10 must be the same as the charging token CTs stored in the financial server 4. If recharging vouchers are still underway between the financial server 4 and the mobile system 1, 10, CTc may also be temporarily smaller than CTs. The financial server 4 therefore checks whether CTc ≤ CTs.

If this condition is not verified in step 240, an unauthorised recharging process has probably been carried out, and the process goes on to step 241. Here it is distinguished whether the fraud was committed by the POT or by the client. If the client is responsible, he is entered in step 242 on a blacklist. A client-barring voucher is preferably generated and sent to the client's mobile system 1, 10 in order to set the blocking flag and block this system, as well as to all POT apparatus, or at least to all POT apparatus in a predefined geographical area, in order to enter this client on the blacklist of these POTs. If, on the other hand, the problem was caused by the POT apparatus, the latter is entered on a POT blacklist in step 243.

If the charging-token test is passed in step 240, the amount A in the transaction voucher may be debited in step 244 to the client's account 41 at the financial institution. Other modes of payment, e.g., via credit card or against an invoice, are naturally also possible within the scope of the present invention. In step 245, the amount A is credited accordingly to an account 420, 420', or 420'' of the POT operator at a financial institution. Service charges may also be debited by a financial institution and/or by the POT operator or by the network operator to the POT account 420 and/or to the client's account 41.

In step 246, the financial server 4 then enters this transaction in the transaction counter. A process then takes place in step 247 for updating the values of the charging token CT and the transaction counter Tc in the mobile system.

Reverting to the process in the mobile system 1, 10, as already explained this system goes to step 248 if a security problem is ascertained in

steps 212, 214, or 216. In this case, a complete check-up takes place with the financial server, preferably via the mobile radio system 6. The check-up comprises, for example, a test and a renewal of the authentication certificate, as well as a verification of all parameters, e.g., the charging token CT, the transaction counter Tc, the blacklist, etc. If the result of the check-up is negative, the blocking flag is set so that the mobile system 1, or at least the respective application in the SIM card 10, is blocked (step 253). If, on the contrary, this check indicates that most probably no fraud has been attempted, the validation time is reset in step 250. By means of the validation time, the mobile system, for example, can be blocked if it is not used within a predefined period of time, e.g., a year. Hence this indication must be reset after each use. The blocking flag is then deleted in step 251, and a new area is set in step 252.

It is important to note that the debiting process may take place with differing currencies, e.g., on the basis of the SDR (special drawing rights) customary in the sphere of telecommunications or by means of some other reference currency (e.g., euros or dollars). The maximum sum of the card is defined according to client class. A default value in SDR is possible as a minimum. Each apparatus 2 stores the SDR value (currency-specific) relevant for it as communicated to it by the server in the log-in process. Depending on exchange fluctuations, the POT apparatus are automatically supplied with current exchange rates by the financial server.

A method of recharging the mobile system 1, 10 with a sum of money will now be described in detail with the aid of Fig. 6. This method can likewise be applied to any of the embodiments of the invention illustrated in Figs. 1 to 4.

A recharging process takes place with the client's mobile system 1, 10 and the POT apparatus 2 together. However, a direct recharging process from the financial server 4 might also be applied. Depending upon the client class, or also according to need, the voucher card stack can be retrieved from the client by the financial server for detailed checking. After the recharging process, the stack can be deleted by the financial server.

The first column in Fig. 6 shows the process steps involving chiefly the mobile system 1; the second column describes the process steps carried out by the POT apparatus 2; the third column relates to the operations of the financial server 4, and the fourth to the effects upon the various accounts at the financial institution. It must be noted, however, that many process steps may be carried out either with the mobile system 1, e.g., within the SIM card 10, or with the POT apparatus 2. For example, the process steps relating to the data input may take place either on the POT apparatus or on the mobile apparatus 1 if the mobile apparatus has a keypad, such as a GSM mobile apparatus. If the mobile apparatus 1 and the POT apparatus 2 are not wire-connected, the communication between the two parts is preferably coded, e.g., by means of a DEA, DES, TDES, RSA, or ECC security algorithm.

In step 300, the mobile system 1, 10, e.g., the identification card 10, is first operatively released for the recharging process; the POT apparatus 2 is also activated in turn in step 301. The POT apparatus 2 then calls up in step 302 in a broadcast process the next, indeterminate mobile system 1, 10 ("card paging").

When the connection between the POT apparatus 2 and the mobile system 1, 10 has been established, the client supplies the POT in step 303 with his IDUI (international debit user identification) and the type of process to be started, here recharging.

The POT apparatus 2 contains a blacklist, preferably updated periodically by the financial server 4, of mobile systems to be barred (revocation list). The IDUI transmitted by the client is compared with the blacklist (step 304). If the IDUI furnished by the client is found on the blacklist (step 305), a blocking flag is set in step 306. Thereafter, or if no entry is found, it is checked in step 307 whether the order correlates with the IDUI. If not, the reason for rejection is displayed on the POT apparatus 2 (step 315). Otherwise, the blocking flag is checked in step 308. If it is set, the mobile system 1, or at least the respective application in the identification card 10, is blocked (step 331). If it is not set, the client is prompted in step 310 to enter his user password manually on the mobile apparatus 1. If the password

entered is not correct (step 311), the blocking flag is likewise set and the reason for rejection displayed on the POT apparatus 2 (step 315); otherwise, the process is free for recharging, and the client is prompted in step 312 to enter the data specific to the transaction, here a recharging amount A. In the modification illustrated, the recharging amount may be entered on the POT apparatus; this amount is linked in step 313 with the POSID and the IDUI, signed, and transmitted to the card 10. However, the amount A might also be entered on the mobile apparatus 1; in that case, no POT is involved, hence the POSID is not needed.

It is checked in step 314 whether the IDUI in the data received by the POT apparatus 2 coincides with the client's own IDUI. If not, the reason for rejection is displayed on the POT apparatus 2 (step 315); otherwise, the desired recharging amount entered on the POT apparatus is displayed on the screen of the mobile apparatus. In step 316, the POSID, the IDUI, the already mentioned number of payment transactions Tc, the number of recharging processes carried out as stored on the card (CTc,), client charging token), and the sum remaining on the card (debit rest amount, DRA) are linked, signed, encoded, and then optionally compressed. A recharging voucher is thereby created. Optionally, the voucher stack on the card may also be transmitted, e.g., according to client class, upon card issuance, or as necessary during use in case of solvency problems. The POSID is now integrated in the recharging voucher if the client has a mobile apparatus without the POT input part so that he can also be addressed by the financial server. The recharging voucher is then transmitted to the financial server 4, 4', or 4", where the TTP server 40, in step 317, receives this voucher, decodes and decompresses it, if need be, and verifies the signature of the client and, as the case may be, of the POT.

With the aid of the table 318, which stores the number and tokens with respect to the processes between the client and the financial server, the following tests are carried out in step 319:

Test of amounts: the sum ΣA of all amounts credited to the card, including the starting sum, must be equal to or less than the sum of all check debits ΣCD and of the remainder DRA on the card. The sum may be less

because the vouchers still underway between the mobile system 1, 10, the clearing unit 3, and the financial server 4, 4', 4" cannot yet be included at this moment.

Charging-token test: the number of charging and recharging transactions is counted in the mobile system, e.g., by means of a token CTc in the SIM card and by means of another token CTs in the financial server 4. These two tokens must be equal.

Transaction-counter test: for each payment transaction, the transaction counter Tc in mobile system 1, 10 is incremented; in each recharging voucher, Tc is also transmitted. The count of the transaction counter Tcs stored at the financial server and incremented by the vouchers transferred by the client must be equal to or possibly less than that of the transaction counter Tc in the mobile system 1, 10.

If one of these three conditions is not fulfilled (step 320), the blocking flag is set in step 321 and the recharging process refused in step 325. Otherwise, the balance of the client's account 41 is checked in step 322. If it does not suffice for recharging, the refusal is likewise prepared in step 325.

If the client's account (or credit limit) at the financial institution 4 suffices for the amount to be recharged (steps 322, 323), this amount is withdrawn from the client's account 41 (324), including any commissions. A recharging voucher is then prepared in step 326 from the POSID, the IDUI, the amount A, the new charging token CTn, and a predefined time-out increment TOi. In step 327 this recharging voucher is signed, optionally encoded and compressed, and transmitted to the client's mobile system 1, 10. During step 328, the latter checks whether the signature in the voucher comes from the financial server and verifies during step 330 whether the blocking flag is set. If so (step 330), the mobile system 1, or at least the respective application, is blocked in step 331. Otherwise, it is checked whether the financial server has called for a rejection (step 332), which leads to interruption of the process with an indication of the reason for rejection (step 334).

If all tests have been successfully passed, the card account is credited in step 335 with the recharging amount called for. The old charging token CTc is then replaced by the new charging token CTn transmitted by the financial server (step 336), the transaction counter Tc on the card is reset in the next step 337, and the time-out TOi is reset in step 338. If it is found in step 339 that the POSID is contained in the recharging voucher, a new area is further set in step 340.

The recharging amount is then displayed by way of confirmation, either on the screen of the mobile apparatus or on the POT apparatus (step 341). Finally, the total balance of the account is also displayed on the card (step 342).

Security of the data transfers by cryptography is differently undertaken in two discrete segments. Between the client and the POT, the communication through the air interface is safeguarded by, for example, an algorithm such as DES, TDES, RSA, or ECC. Between the client and the financial server, on the other hand, the TTP (trusted third-party) method, or optionally a PTP (point-to-point) method, is used. The necessary elements are integrated on the identification element 10 and in the TTP server 40. A description of the TTP concept is appended.

The information flow in a fifth modification of the inventive transaction method will be explained below with the aid of Fig. 7. The client is equipped with a mobile apparatus 1 which likewise contains a SIM card 10 identifying him in the GSM network 5. The seller needs a POT apparatus 2 having a modem connection 22 to a telecommunication network 6, e.g., a fixed network. Both have a contract with the operator of the financial server 4', e.g., a financial institution.

In order for the transaction between client and seller to take place, the seller must first key in on the POT 2 the amount A to be paid. The POT apparatus links this amount A with a POSID stored in the POT and identifying the branch and the cash desk in this branch. These linked data are transmitted to the financial server 4' over the preferably secured data network 6.

The client prepares on his apparatus 1 a special short message, preferably an SMS message, or possibly a USSD file, containing the amount A to be paid and the POSID communicated verbally by the seller, and sends this short message via the GSM network 5 and the short message service centre (SMSC, not shown) to the financial server 4'. This short message automatically contains the client identification stored in the SIM card. Preferably, a requested security PIN code is additionally comprised. The short message may be encoded prior to transmission.

Preferably, no indications concerning the service, product, or information purchased are transmitted in order to protect the buyer's privacy.

The financial server 4' receives the data from the POT apparatus 2 and from the client's mobile system 1 and supplements them, if necessary. It knows the POSID identity and the amount A from the POT. Hence it can determine the POT account 420, 420', 420" to be credited. It knows the identity of the client by means of client identification and, if need be, the PIN and the amount. Hence it can determine the client's account 41 to be debited. The financial server 4' then compares the POSID transmitted by the POT apparatus 2 and by the mobile system, as well as the amount. If they agree, the transaction takes place between the POT account and the client's account. The financial server 4' then sends a message to the POT apparatus 2 and/or to the mobile apparatus 1 that the transaction has taken place, and this message is displayed. In the event of discrepancy, the operation is cancelled.

The information flow in a sixth modification of the inventive transaction method will be explained below with the aid of Fig. 8. The client is equipped with a mobile apparatus 1 which likewise contains a SIM card 10 identifying him in the mobile radio network 5. The seller needs a POT apparatus 2 having a modem connection 22 to a telecommunication network 6, e.g., a fixed network. Both have a contract with the operator of the financial server 4', e.g., a financial institution.

In order for the transaction between client and seller to take place, the operator of the POT apparatus, e.g., a salesperson, must enter on the POT

apparatus 2 the amount A to be paid and the client's mobile telephone number. The POT apparatus links these particulars with a POSID stored in the POT, identifying the branch and the cash desk in this branch. These linked data are transmitted to the financial server 4' over the preferably protected data network 6. Preferably, no information concerning the product purchase is transmitted in order to guarantee the buyer's anonymity.

The financial server 4' receives the data from the POT and supplements them, if necessary. It knows the identity POSID of the POT and the amount A. Hence it can determine the POT account 420, 420', 420'' to be credited. Likewise, it can identify the client by the mobile telephone number transmitted and therefore knows the client's account 41 to be debited.

The financial server 4' then sends the client a special short message, e.g., an SMS or USSD short message, containing the amount A. The client must then confirm the transaction by means of a confirmation short message containing an identification of the client in the GSM network. If no confirmation comes from the client, or if the identification transmitted does not agree with the client's mobile telephone number, the operation is cancelled. Otherwise, the transaction takes place.

The information flow in a seventh modification of the inventive transaction method will be explained below with the aid of Fig. 9. The client is equipped with a mobile apparatus 1 which likewise contains a SIM card 10 identifying him in the GSM network 5. The seller requires a normal POT apparatus 2 which needs no telecommunication connection. Both have a contract with the operator of the financial server 4', e.g., a financial institution.

In order for the transaction between client and seller to take place, the client must prepare a special short message, e.g., an SMS or USSD short message, containing the amount A to be paid and the POSID communicated by the seller, and must send this short message via the GSM network 5 and the SIM centre to the financial server 4'. This short message automatically contains the client identification stored in the SIM card. It preferably further

contains a requested security PIN code. Preferably, no information concerning the purchased product is transmitted in order to protect the buyer's privacy.

The financial server 4' receives the data from the client and supplements them, if necessary. It knows the identity POSID of the POT apparatus and the amount A. Hence it can determine the POT account 420 to be credited. Likewise, it can identify the client through the client identification in the short message and therefore knows the client's account to be debited.

The financial server 4' effects the transaction and sends the POT operator a confirmation in the form of a short message, an E-mail message, or a normal letter by post. This communication contains at least the identification of the POT, the date, the time, the amount, and possibly the client's account.

Preferably, all vouchers are transmitted between mobile apparatus, POT apparatus, and the financial servers as SMS or USSD messages. If SMS messages are used, they are preferably provided with a special header in the data telegram in order to distinguish them from ordinary messages. In addition, the contents of these messages are preferably encoded by means of the TTP method described in the appendix and illustrated by Figs. 10 to 13.

Those skilled in the art will understand that the invention is also suitable for non-financial transactions between a mobile system and a POT apparatus 2 connected to a telecommunication network 5. For example, the POT apparatus 2 may also take the form of a locking device; for this application, the mobile system 10, e.g., in the form of a chip card, has an electronic code loaded; the code is reloaded from the server 4 and stored on the card 10. In order to open the locking device, a contact-free communication is established between the mobile system 10 and the POT apparatus 2, e.g., through an inductive or possibly infrared interface. The locking device is opened only when, after this communication, the code stored in the mobile system 10 proves to be correct and gives its owner the right to enter the protected zone. The server 4, to which the locking device is connected over the network 5, administers and registers the admission permits and, if need be,

debits the client's account 41 for an amount dependent upon the admissions which take place.

Appendix - Basic Principles of Cryptography and TTPs

Security Requirements

In the exchange of data between the mobile system 1, 10 and the financial server 4, a distinction is made among the following requirements for security:

- confidentiality: guarantee that information is not made accessible or legible to unauthorised parties.

- authentication: process in which authenticity is checked.

- authenticity: proof of identify. It provides the certainty that the client, the POT apparatus 2, or the server 4 really is the one it claims to be.

- authenticity of information: certainty that the sender or producer of information (mobile system 1, 10, POT apparatus, or financial server) is authentic.

- undeniability of origin - proof of origin: the sender of information cannot deny that the information comes from him.

- integrity: guarantee of the consistency of the information, i.e., protection against alteration, addition, or deletion of information.

Hereafter the term "message" is used instead of the term "information." A message is information (here a bit sequence) transmitted from a sender to a recipient. For this application, a message may, for example, be a payment voucher or a recharging voucher. The terms "sender" and "recipient"

mean, depending upon the direction of the message, either the mobile system 1, 10, the POT apparatus 2, or the financial server 4.

The authenticity of the sender, integrity of the information, and undeniability of the origin of the information are achieved through the use of a so-called digital signature. A digital signature is a cryptographic key or code (i.e., a bit sequence) unique to certain information and requiring for its production a cryptographic key (also a bit sequence) held only by the author. Consequently, the digital signature can be produced only by the holder of the private key. It is normally added to the original message.

The confidentiality of the information transmission is achieved by encoding. This consists in transforming the message into an illegible condition with the aid of an encoding algorithm and a cryptographic key or code (bit sequence). The original information cannot be recovered from the message thus transformed unless the key necessary for decoding is known.

How this functions in detail is explained below.

Symmetrical and asymmetrical encoding

A distinction is made between two kinds of encoding algorithms:

- symmetrical: the same cryptographic key is used for encryption and decryption (encryption = encoding) of information. Accordingly, the sender and the recipient must be in possession of the same key. Without this key it is impossible to get the original information back again. The symmetrical algorithm used most frequently today is DES (digital encryption standard). Other algorithms are, for example, IDEA, RC2, and RC4. Symmetrical algorithms are preferably utilised for protecting data transfers between mobile system and POT apparatus. The key is then stored in the POT apparatus 2 and in the mobile system 10.

- asymmetrical: two different, complementary keys (key pair) are used for encryption and decryption; this means that the message is

encrypted by means of a first key and decrypted by means of a second key. This procedure is reversible, i.e., the second key can also be used for encryption and the first key for decryption. It is impossible to reconstruct the second key on the basis of the first key (and vice versa). It is equally impossible to calculate the key based upon the encrypted information (this is true even if the original information is known). The asymmetrical algorithm by far most widely used today is RSA (named after its inventors, Rivest, Shamir, and Adleman). A variant of it is DSS (digital signature standard).

With the aid of asymmetrical encryption, a so-called digital signature can be produced. How that functions in detail is explained below.

Private and public keys

With the aid of the asymmetrical encoding technology, a so-called system of public and private keys can be created. Here one key of the complementary key pair is called private. It is held by the sender, e.g., the client, and is known only to him. It is therefore also called the secret key (though this term is normally used for symmetrical keys). The other key is the public key. It is accessible to all. As mentioned above, it is not possible to calculate the private key on the basis of the public key. Each mobile system, POT apparatus, and financial server receives from a trustworthy source a key pair consisting of a private key and a public key.

It is of the greatest importance that the private key really does remain secret, i.e., that it is not known to anyone else, as it forms the basis for the security of the digital signature. For this reason, the private key is stored only in encoded form on the identification card 10, on which, moreover, the encryption algorithm is directly implemented. In this way, the private key always remains in the chip and does not leave it at any moment. The data to be encoded are transferred to the chip, are encoded there, and are subsequently returned. The architecture of the chip is such that the private key can be read neither by electronic means, nor by optical, mechanical, chemical or electromagnetic means.

Contrary to the private key, the public key is generally known and is distributed to all users. For the sake of simplicity, the public key is usually sent along with each message. As will be seen below, a trustworthy authority (certification authority) is needed to guarantee the authenticity of the public key since a criminal could produce his own key pair and pretend to be someone else. This guarantee of authenticity takes the form of a so-called certificate, which will be described in detail below.

The hash function

The hash function is a non-reciprocal algorithm which produces a hash value (abridgment, compressed version) of fixed length. It is comparable to the sum of the digits of a whole number. Here the length of the message is typically somewhat greater than the hash value calculated from it. Thus, for example, the message may comprise several megabytes, whereas the hash value is only 128 bits long. It is to be heeded that the original information cannot be deduced on the basis of the hash value (non-reciprocity) and that it is extremely difficult to alter the information in such a way that it yields the same hash value. The purpose of such a function is the production of a short code unique to the respective document. This code is used for producing the digital signature. Examples of hash algorithms are MD4 (message service 4), MD5, RIPE-MD, and SHA (secure hash algorithm).

The digital (electronic) signature

This method is described with reference to Fig. 10. Every user receives a private key and a public key. In order to sign a message 90 digitally, it is encrypted with the sender's private key (block 94). The result is the digital signature 92. However, since the signature thus created would be the same size as the original message, the hash value 93 of the message 90 is first calculated. As mentioned above, the hash value has a fixed length and is unique to a specific message. For forming the digital signature, the hash value 93 is now encrypted instead of the original message. The digital signature 92 thus created is added to the original document 90. The whole thing is then sent to the recipient (Fig. 10).

Since only the sender of the document possesses his private key 91, only he can produce the digital signature. It is here, too, that the analogy to a handwritten signature then resides. The digital signature has certain characteristics, however, which are not present in a handwritten signature. Thus, for example, it cannot be ruled out in the case of a contract signed by hand that information has been added or deleted unnoticed, which is not possible with a digital signature. Hence the digital signature offers even better security than the traditional handwritten signature.

Checking the digital signature

Since the public key 97 is distributed to all users and is thus generally known, every recipient can check the digital signature 92. To do this, he decrypts the digital signature 92 by means of the sender's public key 97 (block 96 in Fig. 11). The result is the hash value of the original message 90. Parallel to this, the recipient calculates the hash value 95 of the original document 90 which has also been transmitted to him (together with the signature 92). The recipient now compares the resulting second hash value 95 with the hash value 96 decrypted from the signature. If the two hash values agree, the digital signature is authentic.

If the original message 90 was altered during transmission (one bit is enough), its hash value 95 will change as well. Thus, the recipient would find that the hash value 95 he has calculated on the basis of the original message does not agree with the hash value 96 decrypted from the signature, meaning that the signature is not correct. Consequently, with a successful verification of the digital signature, the recipient has the guarantee that the message 90 has not been altered (integrity).

Since only the producer of a signature is in possession of his private key 91, only he can produce the digital signature 92. This means that the recipient who has the digital signature 92 can prove that only the sender could produce the signature (undeniability of the information origin).

Certification of the public key

The digital signature 92 thus makes possible the undeniability of the origin and the guarantee of integrity of a message 90. Now, however, there still remains one security problem, viz., the guarantee of authenticity of the sender's public key 97. For until now, the recipient has no guarantee that the public key 97 actually is that of the sender. Although the signature may be valid, the public key 97 associated therewith might theoretically be fraudulent.

Hence the recipient of a message 90 needs to be certain that the the sender's public key 97, which he holds, really belongs to the proper sender. He can achieve such certainty in various ways. One possibility is that the sender gave him the public key 97 in person at some time. Or the recipient calls the sender and compares, say, the first 10 places of the public key. However, these methods are troublesome and require that the users either already know each other or have previously met.

It would be better if there were an authority which guarantees that a public key belongs to a certain person. This authority is called a certification authority (CA) and guarantees that a specific public key 97 belongs to a specific person. It does so by producing a so-called certificate 98 of the public key 97 (Fig. 12), consisting essentially of the public key and the name of the holder. The whole thing is then signed by the certification authority (signature 98). By means of the certification, the CA therefore ties a public key 97 to a specific sender (client, POT, or server). For all users, a certificate of the public key is issued in this way by the CA. These certificates are accessible to all users.

By checking the digital signature 99 of the sender's certificate as well as the signature 92 of the message itself, the recipient has proof that the message 90 was signed by the person he claims to be (authentication).

It should be noted that the key certificates 98 need not be specially protected since they cannot be forged. For if the contents of the certificate have been altered, the recipient notices this because the sig

99 is no longer correct. And since no one but the CA has the CA's private key, it is not possible for anyone to forge the signature of the CA.

There are various possibilities of disseminating the key certificates 98, 99. One possibility is to send the certificates 98, 99 along with each message.

With the aid of the techniques described above, two clients, POT or servers unacquainted with each other can therefore mutually exchange information in a secure manner.

Distribution of the public key of the certification authority

There now remains one last problem. As described in the preceding chapter, the recipient of a message checks the sender's certificate. For that purpose, he needs the public key of the certification authority. Now, although the CA could certify its own public key, that would not make much sense since it is possible for anyone to generate a key pair and produce a CA certificate himself (with the respective name of the CA). Thus, there is no actual certificate for the public key of the CA. This fact theoretically allows a criminal to pose as the certification authority and thus to produce and distribute false key pairs and certificates. For this reason, the public key of the certification authority must reach the user through a secure channel. The user must be convinced he holds the correct key of the CA.

One solution which immediately presents itself is to store the public key of the certification authority in the user's SIM card. Although that key can be read (unlike the user's private key), it cannot be overwritten or deleted. This is achieved by means of the special architecture of the chip 101.

Transmitting a digitally signed message without encryption: summary

- By means of his private key 91 stored on the card 10, the sender signs the message 90 in order to confirm its origin.

- The original message 90, together with the signature 92 and the signed certificate 98, 99 of the sender, is sent to the recipient (arrow 80).

- The recipient checks the digital signature 92 of the document 90 with the aid of the sender's public key 97 sent along in the sender's certificate 98.

- In addition, he assures himself of the authenticity of the sender's public key 97 by checking the digital signature 99 of the certificate. He uses for this purpose the public key 81 of the certifying authority.

Encryption of the message

In order to ensure the confidentiality of a transmission, i.e., to protect it from inspection by unauthorized parties, the message must be encoded (encrypted). There are theoretically two possibilities of doing this. The message might be encoded by means of the recipient's public key. Since only the recipient is in possession of the associated private key, consequently only he can decode the message. The fact is, however, that the asymmetrical encryption algorithms are very slow as compared with the symmetrical ones.

Therefore, a symmetrical algorithm is preferably used for encryption of the message (Fig. 13). The sender of a message 90 generates a symmetrical key 83, with the aid of which he encodes the message 90. This symmetrical encoding takes only a fraction of the time which would be needed if an asymmetrical algorithm were used. The recipient must know the same symmetrical key. It must therefore be transmitted to him, itself encoded since otherwise a swindler might also read the key 83 during transmission and could decode the received message 86. For this reason, the symmetrical key 83, the so-called session key, is encoded by means of the recipient's public key 84. The encoded session key thus created is also called a token 85. The token 85 therefore contains the symmetrical key 83 used for encryption of the message 90, encoded by means of the recipient's public (asymmetrical) key 84. The token 85 is transmitted together with the encoded message 86, the signature 92, and the certificate 98, 99.

The recipient decodes the token 85 by means of his private key. He thus obtains the symmetrical key 83 needed for decoding the message. Since only he has the private key, only he can decrypt the message.

Transmission of a digitally signed message with encryption: summary

Sender:

- The sender signs the message 90 by means of his private key 91.

- He then encodes the message 90 by means of a symmetrical key 83 generated by him.

- Next, he encodes this symmetrical key by means of the recipient's public key 84. This creates the token 85.

- The original message 90 is then sent to the recipient together with the signature 92, the token 85, and the signed certificate 98, 99.

Recipient:

- The recipient first decodes the token 85 by means of his private key.

- By means of the symmetrical key 83 thereby recovered, he decodes the message 90.

- He now checks the digital signature 92 of the message 90 with the aid of the public key 97 contained in the sender's certificate 98.

- Moreover, he assures himself of the authenticity of the sender's public key 97 by checking the digital signature 99 of the certificate 98.

by the certification authority. For this purpose, he uses the public key 81 of the certification authority.

Revocation list - invalidation of certificates

Let us assume that a client's SIM card, containing his private key 91, is stolen from him. The thief can now use this private key and pose as the victim of the theft, without this being noticed by the recipient. Hence there is need for a mechanism for informing all users that the certificate belonging to the stolen private key 91 is no longer valid. This is done by means of a so-called list of invalid certificates, the above-mentioned certificate revocation list (CRL). It is digitally signed by the CA and published, i.e., it is made accessible to all POT and servers. Therefore, every recipient of a message from a client, besides verifying the sender's signature and certificate, must now check whether the latter is to be found on the revocation list, i.e., whether it is invalid.

So that the revocation list may not grow too long, only the serial number and the date on which the certificate was invalidated are inserted rather than the whole certificate. The list therefore consists of serial numbers and invalidation dates, digitally signed at the end by the CA. Also given are the date of publication of the list and the name of the CA.

The trust center and trusted third-party services

As shown above, in an open and widespread system of many users in which two users having no joint confidential relationship want to communicate safely with one another, there is need for a third entity which places certain security services at the disposal of such users, for otherwise the time and trouble of exchanging and administering the necessary keys becomes too great for the users. This entity is called a trust center or trusted third party (TTP), and the services it offers are called TTP services. The CA, for instance, is such a service. The TTP takes over the tasks of key administration for the users and therefore enjoys their confidence. The purpose of TTP services is therefore to safeguard various applications and protocols.

The components of a trusted third party are:

- registration authority (RA): it identifies the users, receives their data, and forwards them to the certifying authority. Identification of the users is necessary since the CA guarantees that a specific public key belongs to a specific person. For that purpose, however, this person must first identify himself.

- certification authority (CA): it produces the key certificates and revocation lists. These are then filed in a directory for publication or sent directly to the user.

- key-generating service: it generates the keys for the users. The private key is furnished to the user via a secure channel, the public key is sent to the CA for certification.

- key-personalization service: it files the private keys in a module (e.g., a chip card) to protect them against unauthorized access.

- key-deposit service (key escrow): it stores a copy of the key used (for return in case of loss or for "tapping" by the police on grounds of national security or combating crime).

- file service: it files the key certificates (as a long-term guarantee of digital signature verification).

- directory service: it makes key certificates and revocation lists available to the users.

- notarial services for

1. proof of sending and receipt

2. time stamp

3. attestation of correctness of contents (analogous to existing notarial services)

The procedures described above often state that "the recipient checks the signature" or "the sender encodes the message." Naturally, the user normally need not explicitly carry out all these functions himself, but rather the mobile system 1, 10 or the financial server 4 does it for him automatically.

Claims

1. A transaction method between a client and a fixed point-of-transaction apparatus (POT apparatus) (2), the method comprising the transmission of at least one client identification, one POT apparatus identification (POSID), and transaction-specific data (A) to a server (4) connected by a telecommunication network (5) to said POT apparatus (2), wherein the POT apparatus identification (POSID) is read or entered in the POT apparatus (2) and transmitted to the server (4) via said telecommunication network (5),

wherein the client is equipped with a portable identification element (10) which contains at least one processor (100, 101) and can co-operate functionally with a mobile apparatus (1; 24) for sending and/or receiving short messages via a mobile radio network (96),

and wherein the client identification is stored in the memory of the identification element (10) and is transmitted via at least one contact-free interface (101-20; 6) to the server (4).

2. A transaction method according to claim 1, characterised in that the client identification (IDUI) and/or the POT apparatus identification (POSID) are first transmitted via a contact-free interface (101-20) between the identification element (1, 10) and the POT apparatus (2) and then linked together with transaction-specific data (A) in an electronic transaction voucher which is transmitted via said telecommunication network (5) to said server (4).

3. A transaction method according to claim 2, characterised in that the identification element (10) is a SIM card.

4. A transaction method according to claim 2, characterised in that the identification element is a transponder (10'), and that the mobile apparatus (24) is contained in the POT apparatus (2).

5. A transaction method according to claim 4, characterised in that the client identification (IDUI) is read in the transponder (10'), is transferred via said contact-free interface (101-20) to the POT apparatus (2"), and is linked in the POT apparatus with a POT apparatus identification (POSID) and with said transaction-specific data (A) in the transaction voucher transmitted to said server (4).

6. A transaction method according to claim 2, characterised in that the identification element (10, 10') communicates with the POT apparatus (2) via an integrated coil.

7. A transaction method according to claim 3, characterised in that the SIM card (10) communicates with the POT apparatus (2) with the aid of a coil integrated in the mobile apparatus (1).

8. A transaction method according to claim 3, characterised in that the SIM card (10) communicates with the POT apparatus (2) with the aid of an infrared transceiver integrated in the mobile apparatus (1).

9. A transaction method according to claim 2, characterised in that at least certain data transmitted via said contact-free interface (101-20) between the POT apparatus (2) and the identification element (10, 10') are encoded.

10. A transaction method according to claim 2, characterised in that the transaction vouchers transmitted by said telecommunication network (5) are encoded.

11. A transaction method according to claim 9, characterised in that the transaction vouchers transmitted by said telecommunication network (5) are not decoded during transmission.

12. A transaction method according to claim 11, characterised in that the transaction vouchers (90) are encoded by means of a symmetrical

algorithm, the symmetrical algorithm using a session key (83) encoded by means of an asymmetrical algorithm.

13. A transaction method according to claim 10, characterised in that the transaction vouchers transmitted by said telecommunication network (5) are certified.

14. A transaction method according to claim 13, characterised in that the transaction vouchers transmitted by said telecommunication network (5) contain an electronic signature of the identification element (10) verifiable by the server.

15. A transaction method according to claim 14, characterised in that the transaction vouchers transmitted by said telecommunication network (5) contain an electronic signature of the POT apparatus (2) verifiable by the server.

16. A transaction method according to claim 10, characterised by the following steps:

producing the hash value (93) from the transaction vouchers (90),

encrypting this hash value (93) by means of a private key (91) stored on the identification element (10),

signing the transaction vouchers (90) with the encrypted hash value (92).

17. A transaction method according to claim 2, characterised in that the transaction vouchers are transmitted to the server (4) via a clearing unit (3).

18. A transaction method according to claim 17, characterised in that the data elements (IDUI) needed for clearing in said clearing unit

not encoded, so that the clearing unit need not decode the transaction vouchers.

19. A transaction method according to claim 2, characterised in that the transaction-specific data (A) are read or entered in the POT apparatus (2).

20. A transaction method according to claim 2, characterised in that the transaction-specific data (A) are read or entered in the mobile apparatus (1).

21. A transaction method according to claim 2, characterised in that the server (4) stores a client blacklist, and that the process is interrupted if the client identification (IDUI) received is contained in the client blacklist.

22. A transaction method according to claim 2, characterised in that the server (4) stores a POT blacklist, and that the process is interrupted if the POT apparatus identification (POSID) received is contained in the client blacklist.

23. A transaction method according to claim 2, characterised in that the POT apparatus (2) stores a client blacklist updated by the server (4), and that the process is interrupted if the client identification (IDUI) is contained in the client blacklist.

24. A transaction method according to claim 21, characterised in that the identification element is blocked at least partially if the client identification is contained in a client blacklist in the POT apparatus and/or in the server (4).

25. A transaction method according to claim 2, characterised in that the identification element (10) contains a stack with data concerning transactions already carried out, and that these data can be retrieved by the server (4).

26. A transaction method according to claim 15, characterised in that the transaction-specific data contain an amount of money (A), that the server (4) is administered by a financial institution, and that a sum of money stored on the identification element (10) is debited during the transaction.

27. A transaction method according to claim 26, characterised in that the sum of money stored on the identification element (10) can be recharged over said mobile radio network (6) by means of recharging vouchers from the server (4).

28. A transaction method according to claim 26, characterised in that the amount of money (A) is indicated in a standard currency.

29. A transaction method according to claim 2, characterised in that the transaction-specific data from the POT apparatus (2) are transmitted to the server (4) via a different contact-free interface than the transaction-specific data from the mobile system (10).

30. A transaction method according to claim 4, characterised in that at least certain data from the server (4) are transmitted by a mobile radio network (6) to the mobile apparatus part (24) of the POT apparatus (2") and are relayed from the latter into the transponder (10").

31. A mobile system (1, 10; 10') which can be used for carrying out a transaction method according to one of the preceding claims, containing:

- at least one processor (100, 101) having a memory area in which a client identification (IDUI) is stored,

- electronic reception means for receiving special short messages transmitted over a mobile radio network (6),

- electronic signing means for providing transaction vouchers containing at least the client identification (IDUI) with an electronic signature,

- a contact-free interface (101) for relaying the signed transaction vouchers to a POT apparatus (2).

32. A mobile system according to claim 31, characterised in that the electronic reception means comprise a mobile apparatus (1) and a SIM card (10).

33. A mobile system according to claim 32, characterised in that the contact-free interface comprises an infrared and/or inductive transceiver in the mobile apparatus (1).

34. A mobile system according to claim 31, characterised in that it consists of a transponder (10''), and that the contact-free interface comprises an inductive transceiver.

35. A mobile system according to claim 32, characterised in that the SIM card (10) is a value card.

36. A mobile system according to claim 32, characterised in that said signing means comprise the following elements:

- a private key (91) stored in said memory,

- means for producing a hash value (93) from an uncoded transaction voucher (90),

- means for encrypting the hash value (93) by means of said private key (91) and for signing the transaction voucher with the encrypted hash value (92).

37. A clearing unit (3), characterised in that it receives transaction vouchers from a region, assigns them to the appropriate financial institution (4) as a function of a client identification (IDUI) contained therein, and forwards them to this financial institution.

Abstract

The transaction method between a client and a terminal (2) connected to a telecommunication network comprises the transmission of at least one client identification (IDUI), a terminal identification (POSID), and transaction-specific data (A) to a financial server (4) connected to the telecommunication network. The terminal identification is read or entered in the terminal and transmitted by said telecommunication network to the financial server. The client is equipped with a SIM card (10) which can be connected functionally to a mobile apparatus. The client identification transmitted to the financial server is read in the memory of the SIM card and transmitted to the financial server via at least one air interface.

(Fig. 1)

FIG. 1

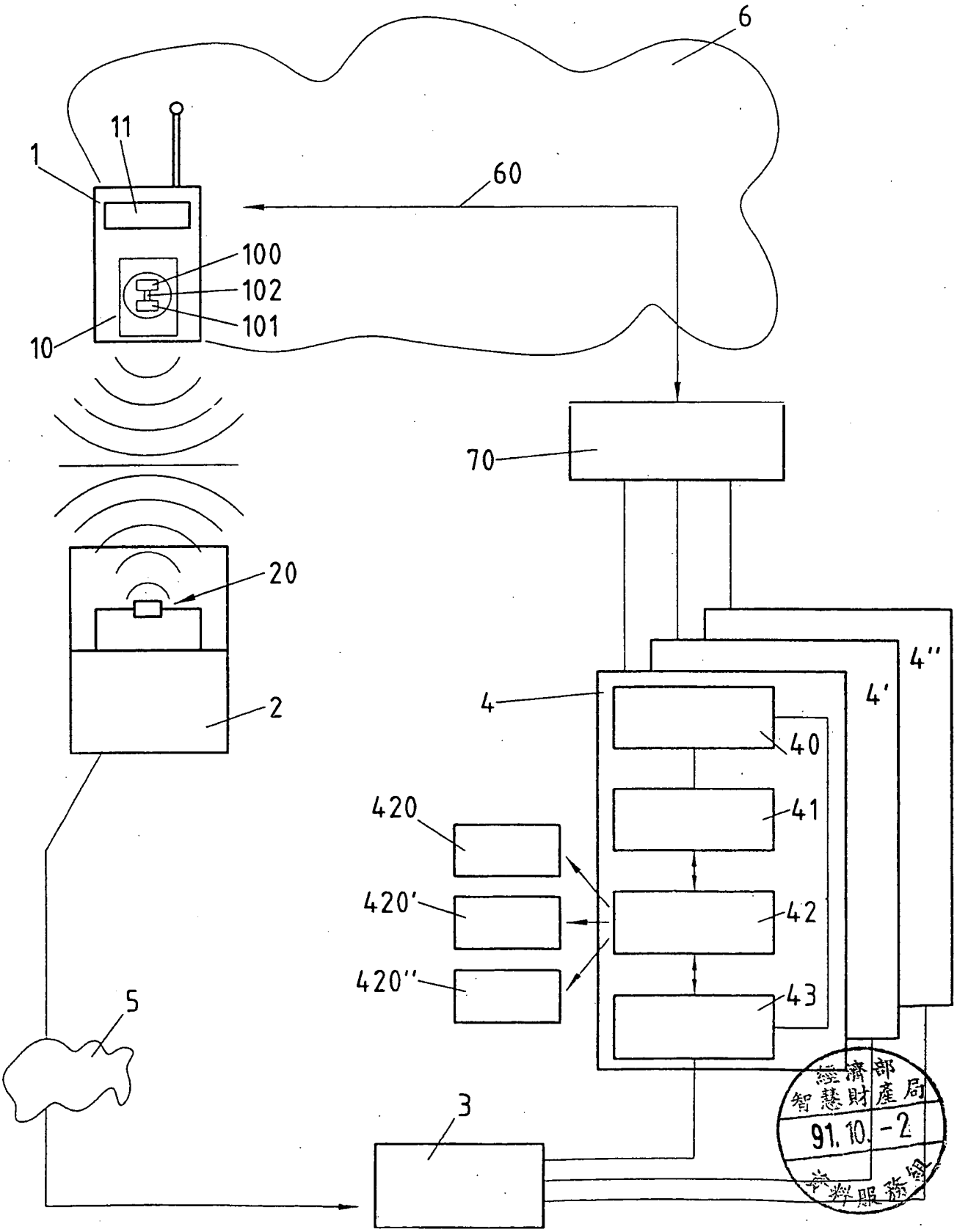


FIG. 2

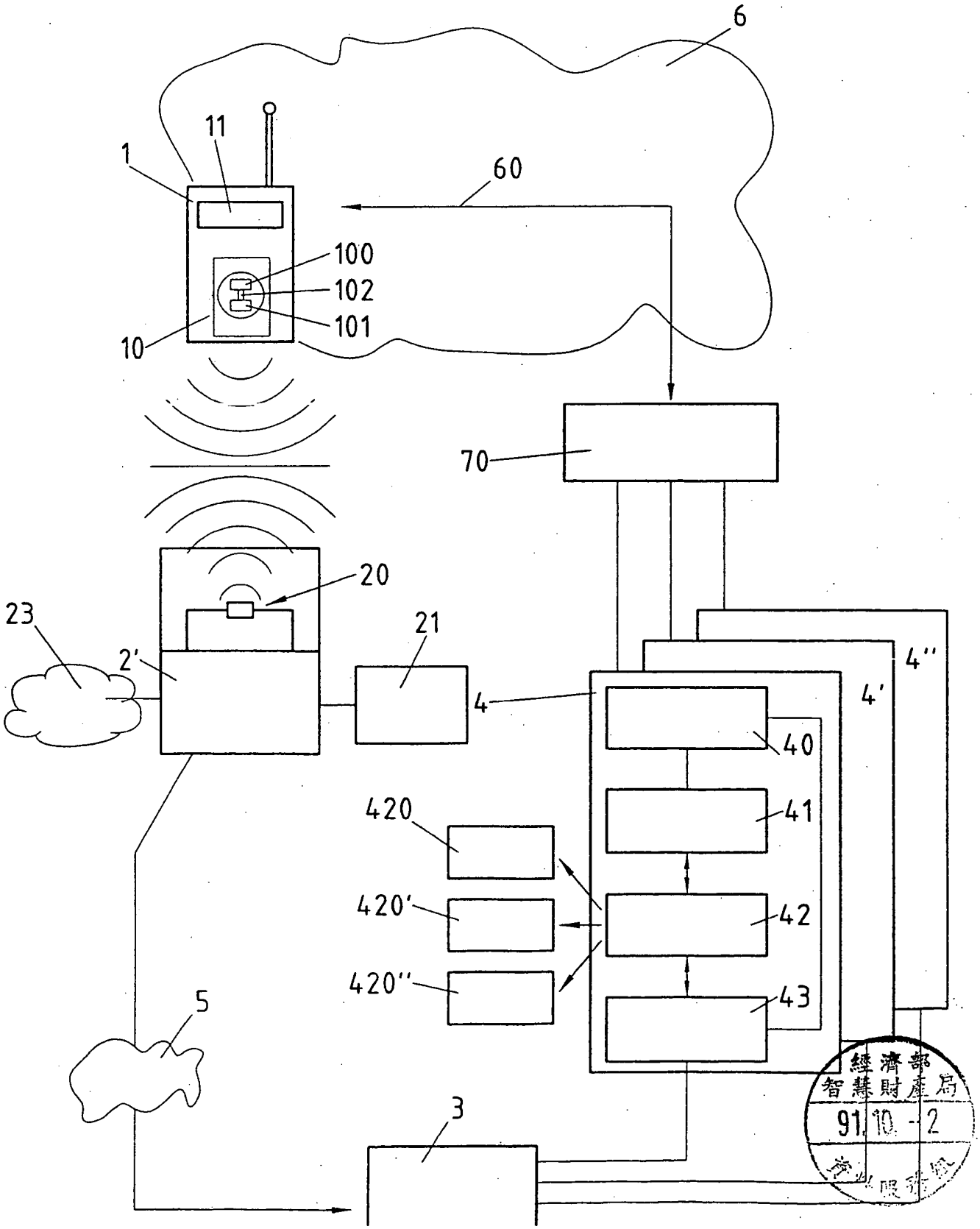


FIG. 3

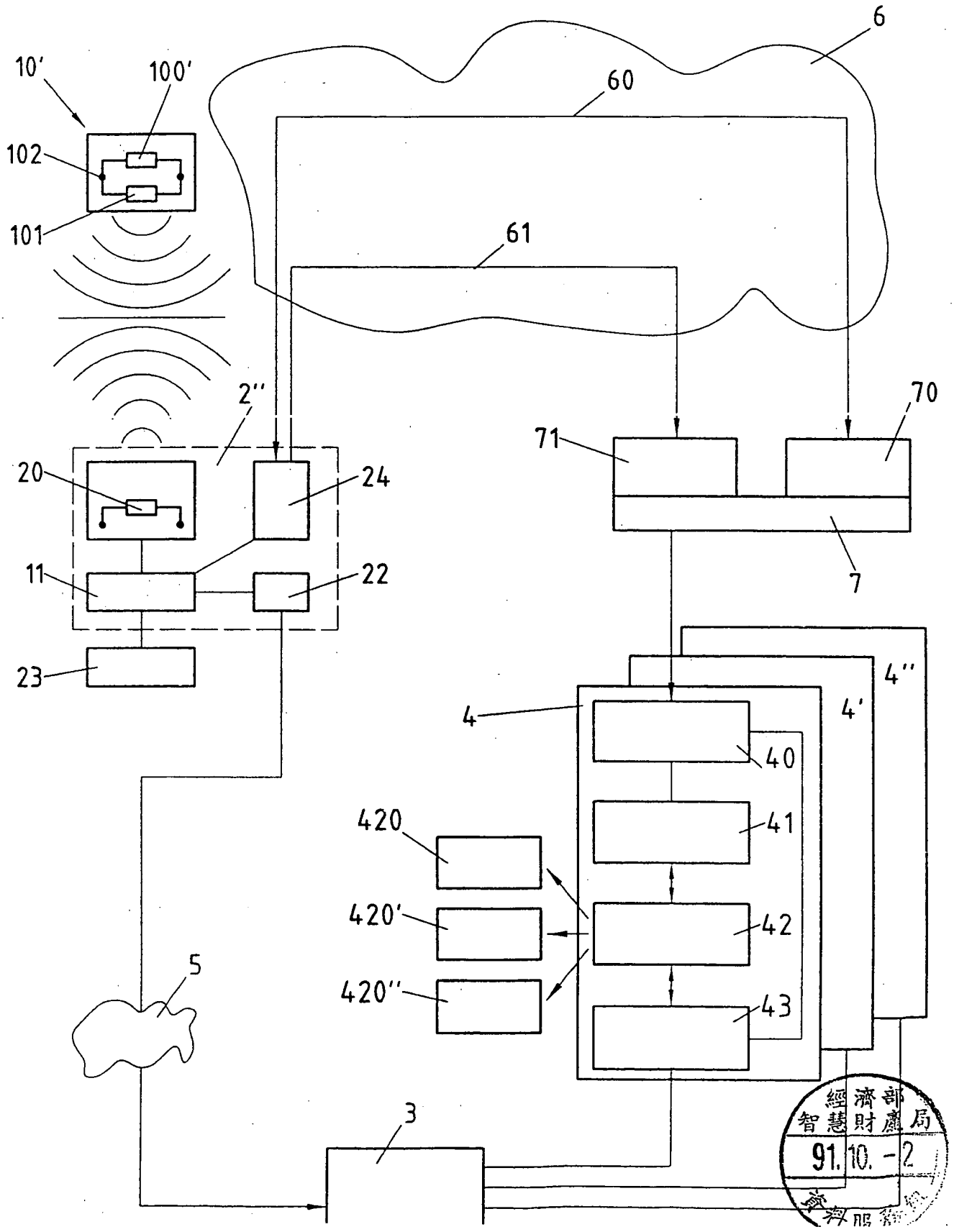
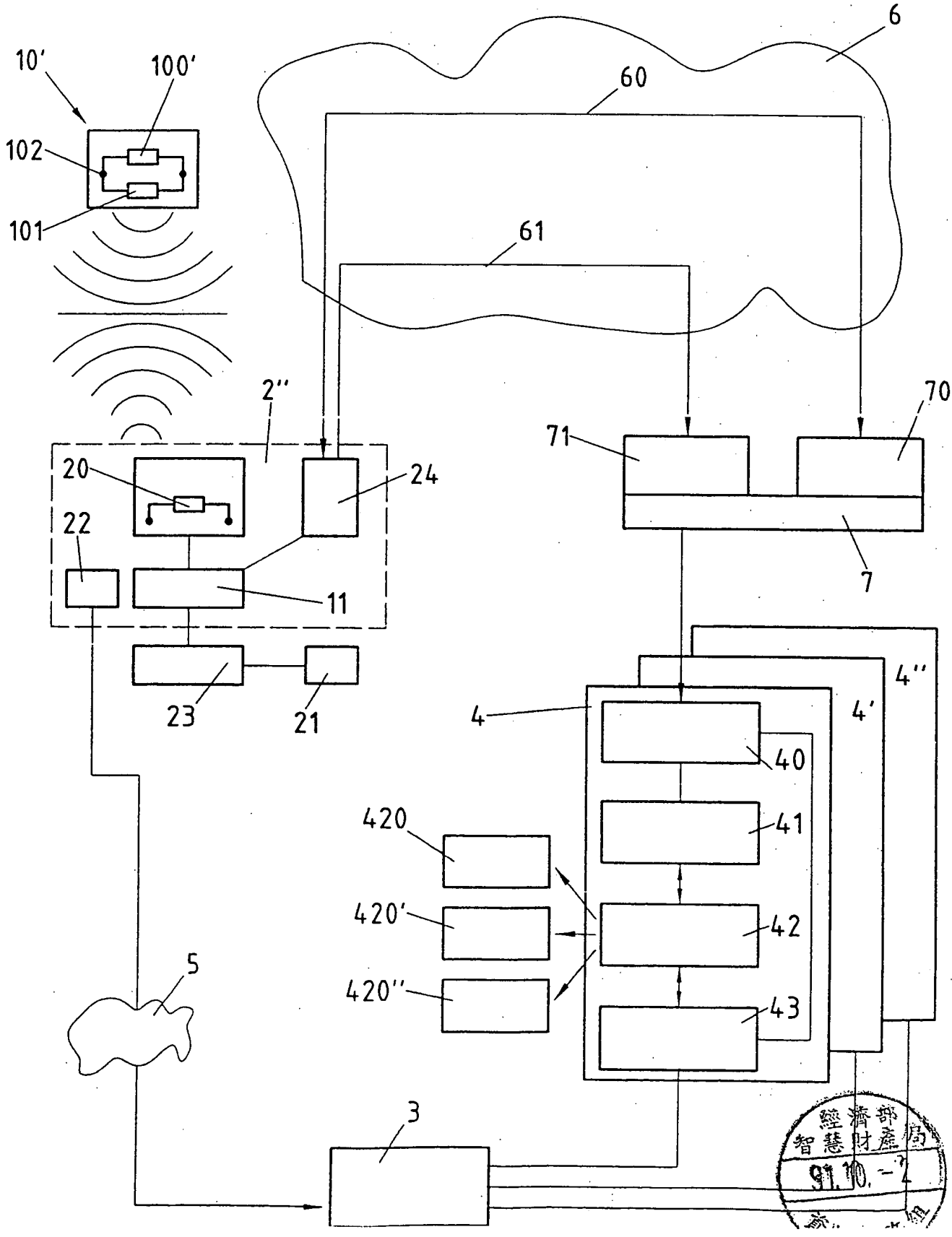
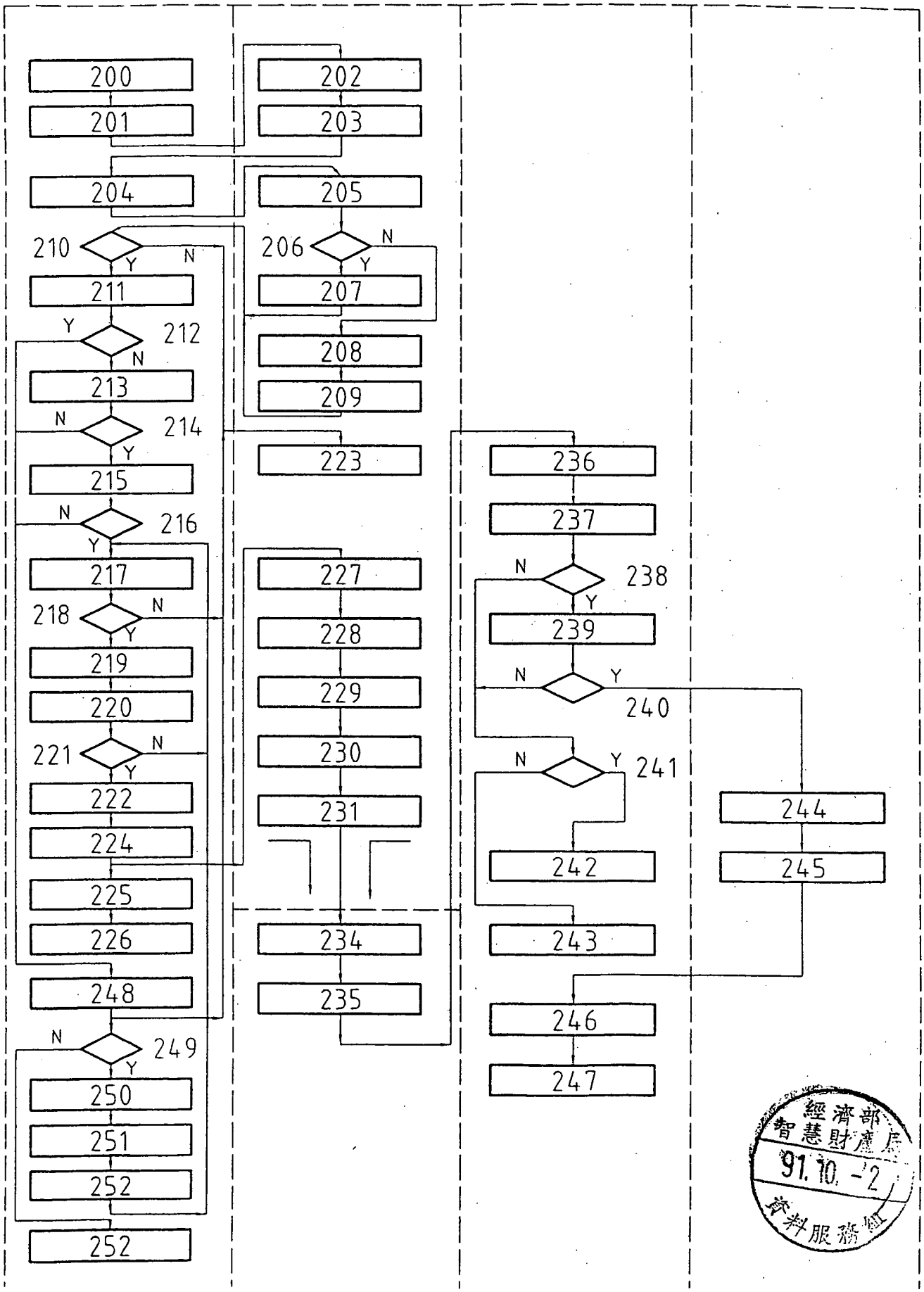


FIG. 4





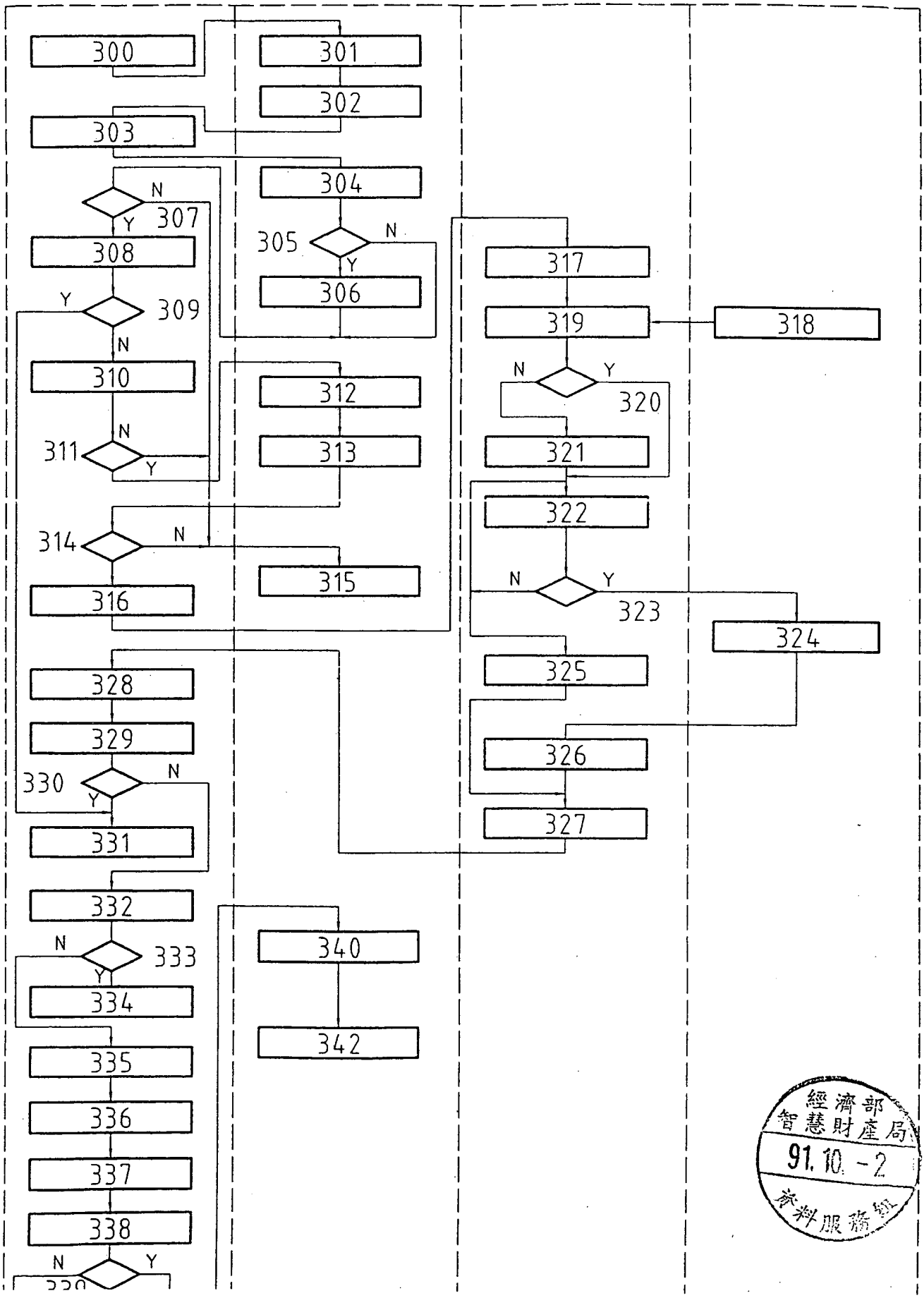


FIG. 7

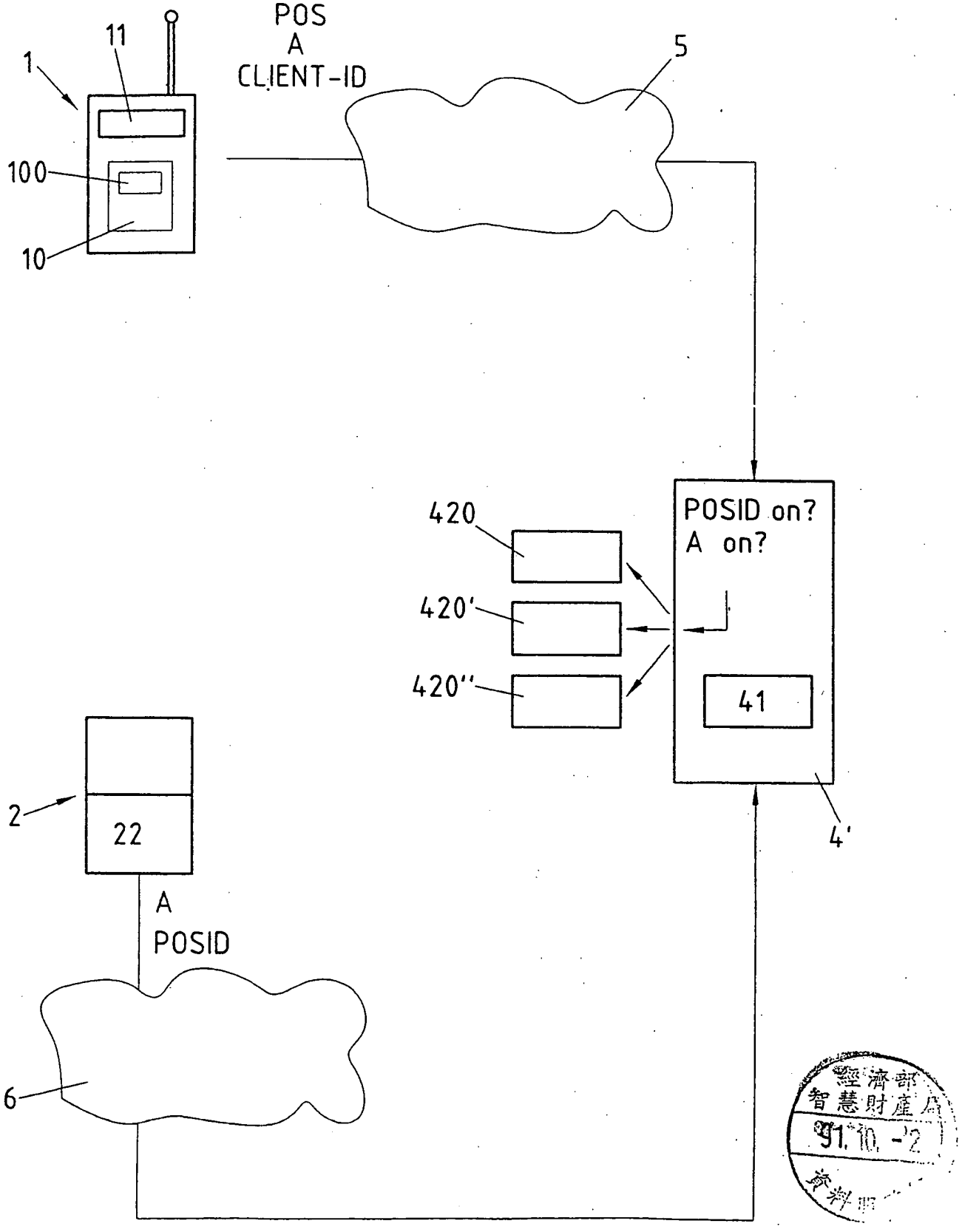


FIG. 8

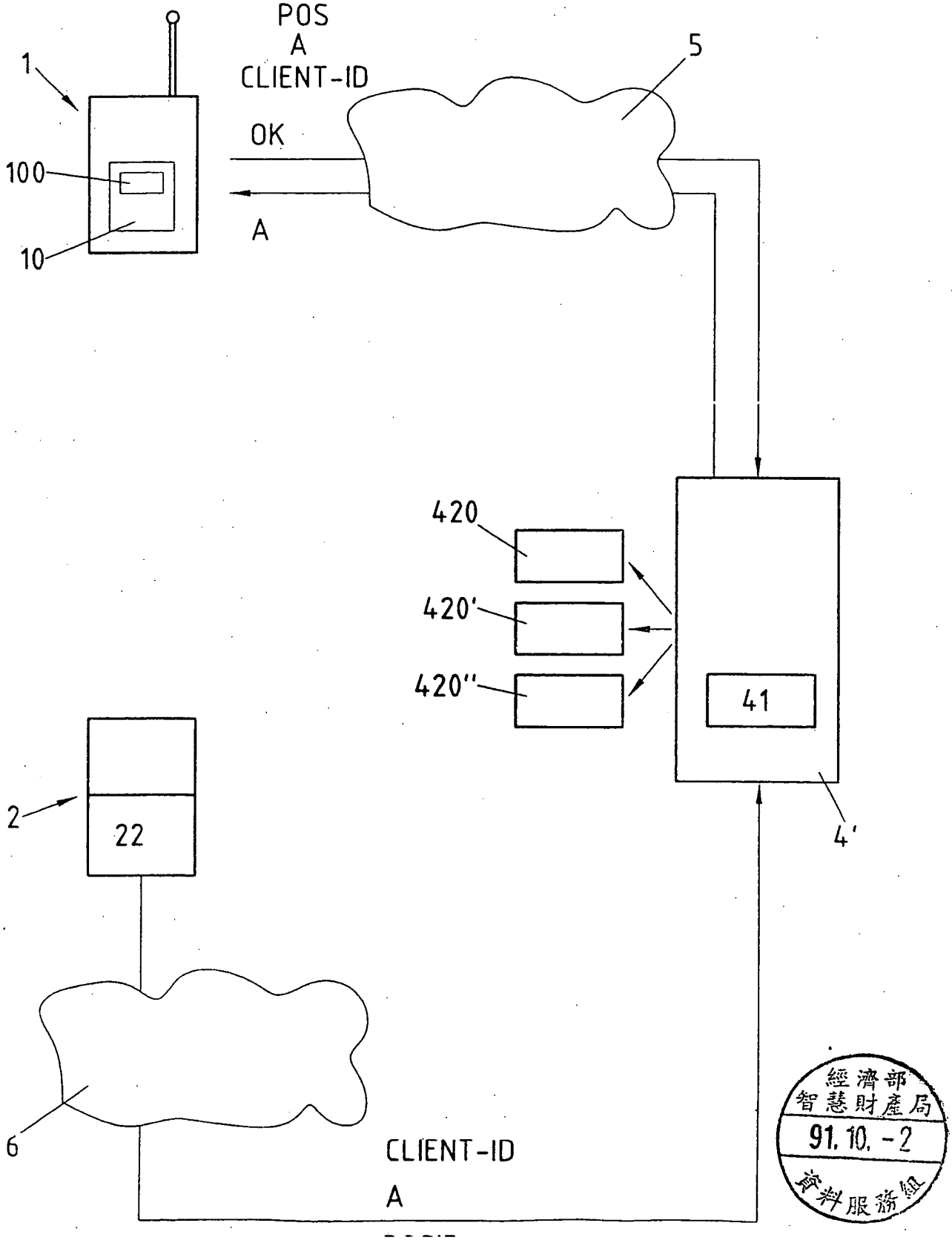


FIG. 9

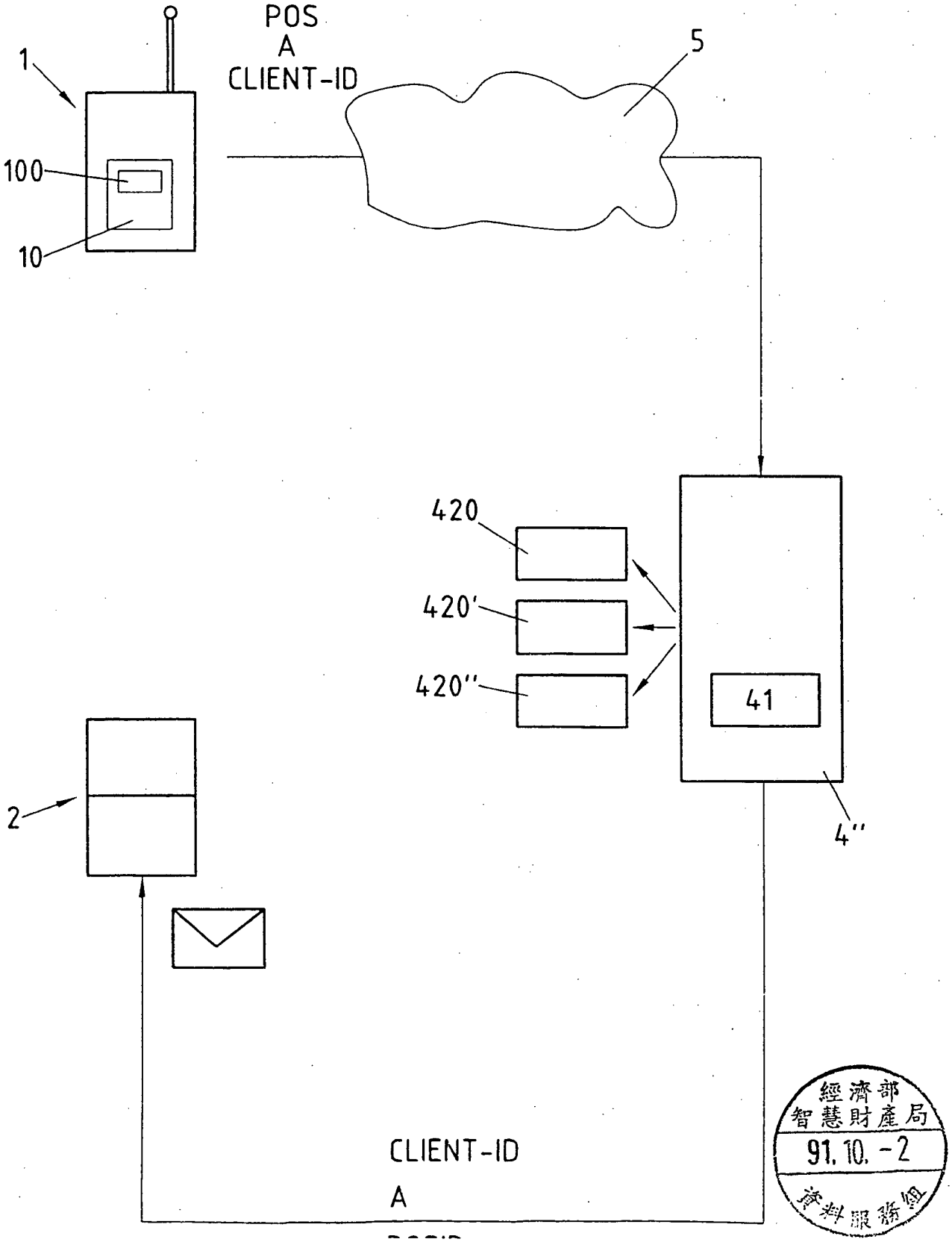
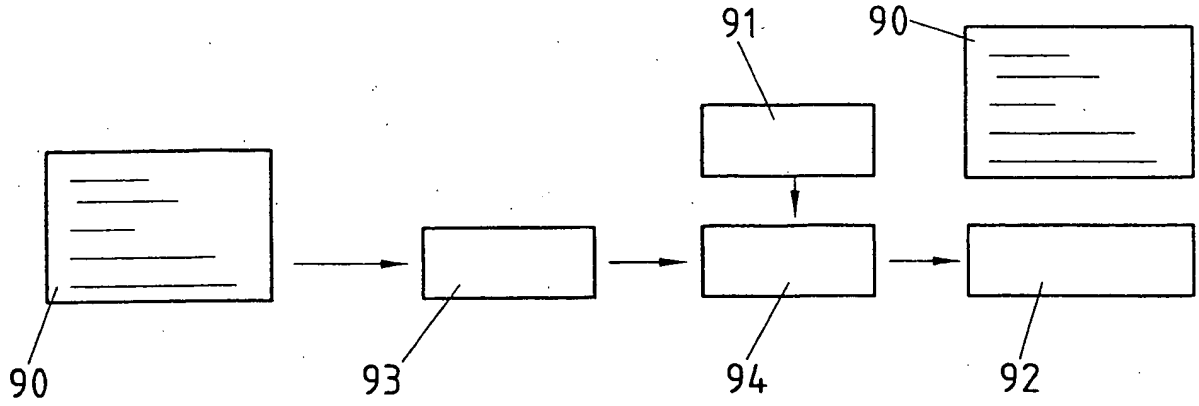


FIG.10



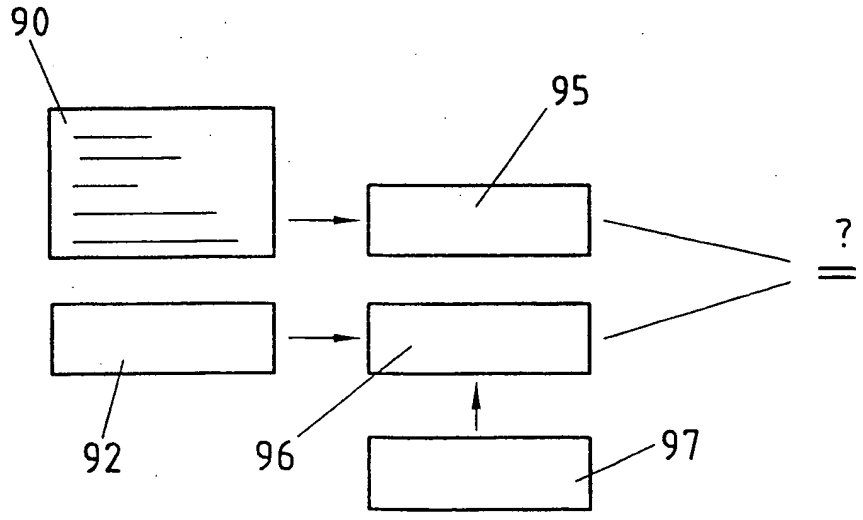


FIG. 11

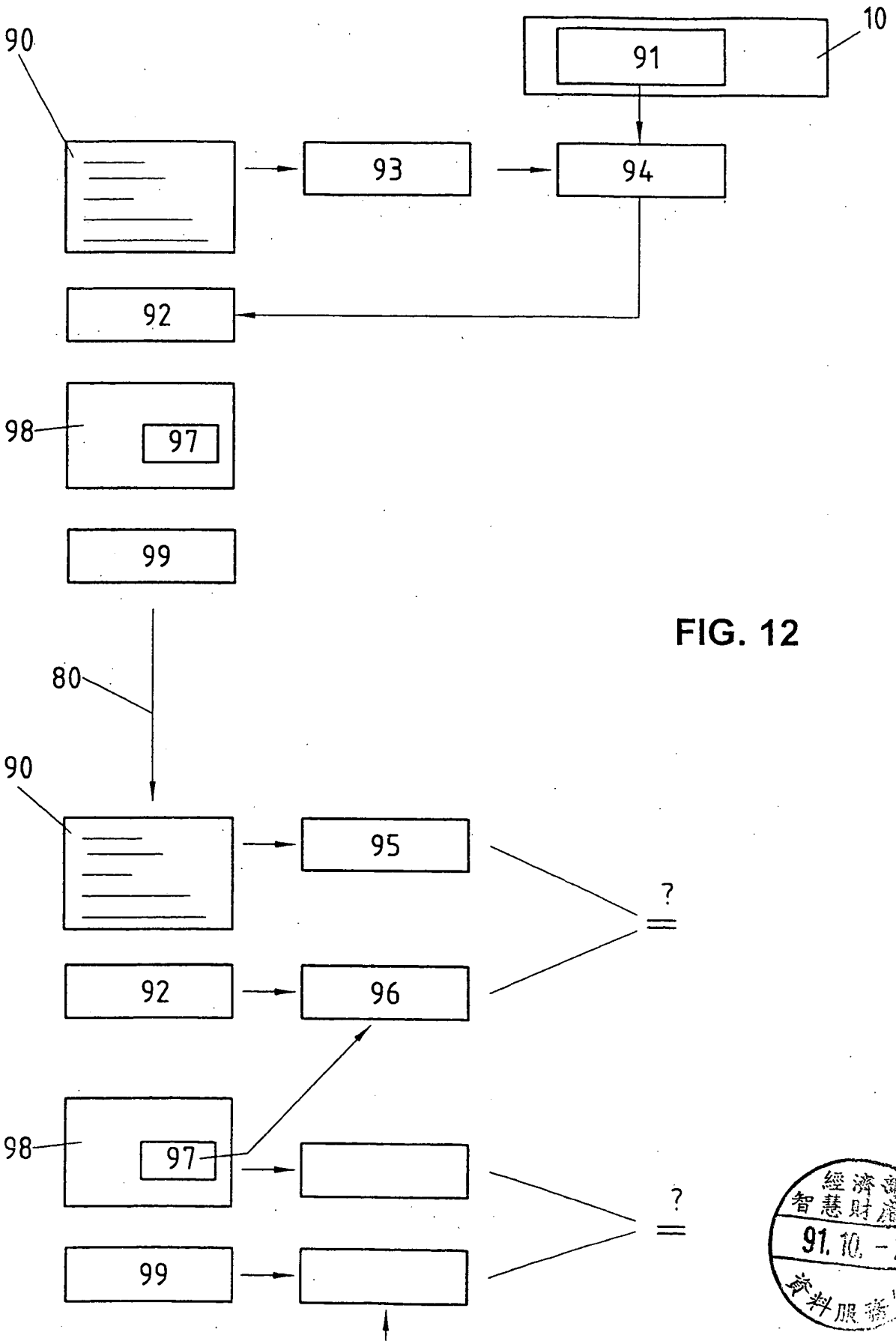


FIG. 12

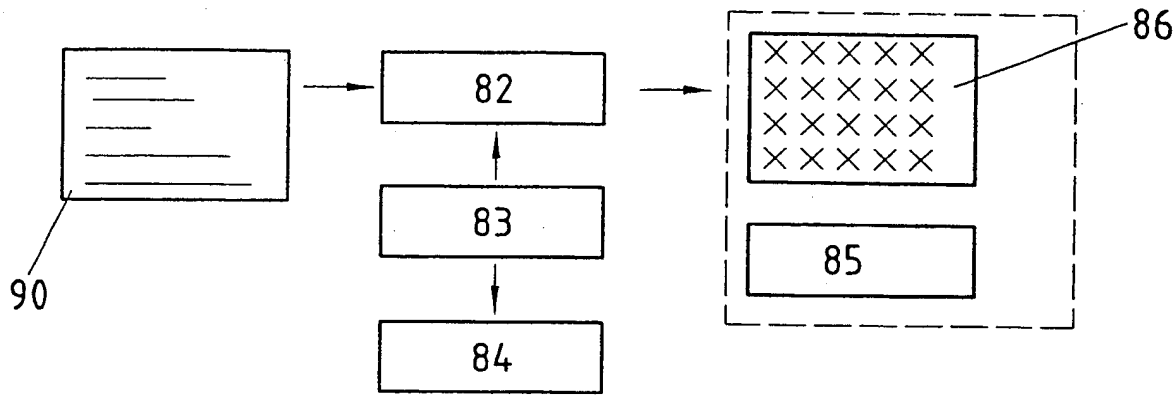


FIG. 13

Patent

Patent No	351799	**Publication Date**	1999/2/1
Application No	87107650	**Filing Date**	1998/5/18
Title	Transaction method with a mobile apparatus		
IPC	G07G1/14 & G07F19/00		

Author / Inventor

RITTER, RUDOLF (CH) ¡F

Applicant

Name	**Country**	**Individual/Company**
SWISSCOM AG	CH	Company

Patent Abstract

A transaction method between a client and a terminal (POT device) (2) comprises the transmission of at least one client identification, a POT identification (POSID) and transaction-specific data (A) to a server (4) connected to the communication work, the POT identification (POSID) is read or entered in the POT terminal (2) and transmitted by said telecommunication to the server (4) in which the client is equipped with a portable SIM card (10) including a mini processor (100,101) which can be connected functionally to a mobile apparatus (1, 24) and operable together to receive and/or transmit short message via mobile radio network (6), and the client identification transmitted to the server is read in the memory of SIM card (10) and transmitted to server (4) via at least contact interface (101-20,6)

BACK